Cloud to cloud data migration using self sovereign identity for 5G and beyond

M. G. Aruna¹ · Mohammad Kamrul Hasan² · Shayla Islam³ · K. G. Mohan⁴ · Preeta Sharan⁵ · Rosilah Hassan²

Received: 24 June 2021 / Revised: 27 September 2021 / Accepted: 30 October 2021 / Published online: 15 November 2021
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

The Coronavirus pandemic and the work-from-anywhere has created a shift toward cloud-based services. The pandemic is causing an explosion in cloud migration, expected that by 2025, 95% of workloads will live in the cloud. One of the challenges of the cloud is data security. It is the responsibility of cloud service providers to protect user data from unauthorized access. Historically, a third-party auditor (TPA) is used to provide security services over the cloud. With the tremendous growth of demand for cloud-based services, regulatory requirements, there is a need for a semi to fully automated self sovereign identity (SSI) implementation to reduce cost. It's critical to manage cloud data strategically and extend the required protection. At each stage of the data migration process, such as data discovery, classification, and cataloguing of the access to the mission-critical data, need to be secured. Cloud storage services are centralized, which requires users must place trust in a TPA. With the SSI, this can become decentralized, reducing the dependency and cost. Our current work involves replacing TPA with SSI. A cryptographic technique for secure data migration to and from the cloud using SSI implemented. SSI facilitate peer-to-peer transactions, meaning that the in-between presence of TPA needs no longer be involved. The C2C migration performance is recorded and found the background or foreground replication scenario is achievable. Mathematically computed encrypted and decrypted ASCII values for a word matched with the output by the algorithm. The keys generated by the algorithm are validated with an online validator to ensure the correctness of the generated keys. RSA based mutual TLS algorithm is a good option for SSI based C2C migration. SSI is beneficial because of the low maintenance cost, and users are more and more using a cloud platform. The result of the implemented algorithm shows that the SSI based implementation can provide a 13.32 Kbps encryption/decryption rate which is significantly higher than the TPA method of 1 Kbps.

Keywords Transport layer security (TLS) · Third-party auditor (TPA) · Self-sovereign identity (SSI) · Cloud migration · Public key infrastructure (PKI) · Certificate authority (CA) · Registration authority (RA) · Certificate management system · Revocation services · Digital signature

1 Introduction

The security of cloud data depends on the trusted public keys. There are several methods to generate a trusted public access key, such as SSL (secure socket layer) and TLS (transport layer security). The TLS is a matured peer

to peer communication standard over the web. The reliability of TLS can be reduced by a malicious attack that takes advantage of gaps in TLS use. One such scenario is the public-key infrastructure (PKI) that TLS deploys. A single trusted entity can impersonate any website. Conventionally, a trusted certification authority (CA) validates a public key (TLS PKI) [1]. To issue a certificate of authentication, CA is to verify a binding between an identity and a public key. Unfortunately, due to various reasons, this process does not provide a high level of trust in security. The identity verification is over the internet utilizing the trust on the first use model [2]. For each

Extended author information available on the last page of the article

certificate, this verification takes place once (i.e., per certificate issuance). Therefore, an attacker getting a chance to impersonate a domain for just a limited duration can manage to get a domain authentication certificate. In recent times there is ample evidence that even a single CA can result in a successful impersonation attack [3–11]. One of the initial researches suggests preventing such an attack can be done using a new notary system [12]. The driving thought for such an application is to rely on a safer agency, known as a notary. A TLS client refers to a notary for its confirmation about the server's public key. Hence, the client gets the required authorization of the access key [13]. However, this approach had its limitations, such as TLS clients publish details of computers they want to connect, increase the latency of TLS connections [14]. In this paper, we are presenting SSI, an emerging TLS based service that eliminates several issues of the notary-based authentication systems. SSI is leveraging the properties of a blockchain platform. The proposed method achieves transparency, provides a framework for service-level agreement (SLA) enforcement, and relaxes availability requirements. The recent work of S. Khan, et al. on attack-resilient TLS certificate transparency has motivated further research [15]. A secure transmission on the cost of computation and routing overhead is a problem for 5G/6G. Data privacy in 5G/6G networks is driving a distributed and data reliability model for mobile edge-based sensor-cloud (DDR-ESC) [16]. In another work, the authors suggested using fuzzy logic for a network to protect mobile traveler's information in IoT [17].

This work is about finding a replacement of TPA with SSI. The proposed cryptographic technique is using a secure data migration to and from the cloud using SSI. In the proposed approach, peer-to-peer transactions can happen without TPA. Next section a detailed literature survey is presented to provide context about this work.

2 Literature survey

Moghaddam et al. [18] proposed a new intelligent migration approach by utilizing an optimized placement method and delaying migration time based on future resource demand prediction. They developed an algorithm that reduces the number of migrations.

The works [19] is on efficient probabilistic public key encryption (EPPKE) optimized with covariance matrix adaptation evolution strategies (CMA-ES). This approach confirms data integrity by using the Luhn algorithm with BLAKE 2b encapsulation. Compared to the existing processes, the outcome is better. Cloud security is a priority of the industry rather than a trend. Till 2019 most of the organizations rely on the security service which their cloud

service providers (CSP) offer. The scenario of cloud use has been changed, addition to the security what the CSP's are providing, most of the organizations are now very keen on building their strong security foundation for their workloads in the cloud.

The survey paper of Masdari and Khezri [20] is relying on migrations using forecasting techniques in cloud computing. Extensive survey and taxonomy of the predictive migration approach adapted for the cloud data centers. In addition, this paper provides a comparison of the predictive migration schemes and future research areas.

Ahmad et al. [21] presented the strategies and methods for transformation to the cloud computing environment from a client-server-based environment. Also, the authors evaluated the existing cloud migration processes and software available from existing cloud system integrators and operators.

Zhao et al. [22] presented a security-service-level-agreement (SSLA)-guaranteed service function chain deployment in cloud-fog computing networks. They proposed a minimal-cost and SSLA guaranteed service function chain (SFC) deployment algorithm to minimize the cost while satisfying the SSLA. The results show that the blocking ratio and the deployment cost of the algorithms are better than that of the existing algorithm when meeting the SSLAs.

For SSI implementation, the decentralized approach of blockchain is an important feature to consider. We explored Kumar et al. [23] work on blockchain and its application. In this paper, the author presented ideas about blockchain technology and its recent applications. Keys offerings are segregated, unambiguous, publicly verifiable ledger of the transactions.

Casino et al. [24] presented an article with a detailed state-of-the-art research study on blockchain implementations. This article discussed a theoretical understanding of numerous research work published during the last decade. The article discussed the different classifications of blockchain systems.

Chaudhry et al. [25] published research on cloud IoT-based sensor nodes and proposed lack-IoT to implement direct device-to-device communication without using intermediate agents. The reliable access control method was found to reduce the computational time and communication cost. Security was provided using either a formal and informal scheme.

Mo et al. [26] considered IoT sensor node reliability in a cloud system. The work was based on graph decomposition vertices for evaluating the K-terminal. The proposed method underlined issues and challenges in IoT data migrated to cloud systems.

Ahmed et al. [27] proposed optimizing energy consumption using genetic algorithms for IoT data migration

to a cloud system. The proposed method was compared with existing algorithms and results showed a reduction in energy consumption.

The study by Ghazal et al. [28] provided a review highlighting issues, challenges and solutions for security threats and vulnerabilities when transmitting IoT data to cloud systems. Similarly, the work carried out by Liang et al. [29] presented a detailed discussion of different attacks which lead to trust in IoT devices and cloud systems. The proposed trust model was analyzed theoretically, and the results were positive. Wang et al. [30] investigated the issues associated with data privacy in sensor-cloud systems. This study showed that privacy-based mechanisms associated with communication complexity can reduce bandwidth and storage costs. After this survey, we would like to state that the General Data Protection Regulation (GDPR) imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The basic data protection principles governing GDPR are:

- Lawfulness, fairness and transparency,
- Purpose limitation,
- Data minimization,
- Accuracy,
- Storage limitation,
- Integrity and confidentiality,
- Accountability.

Further, the study continued for authentication literature in 5G. Patel et al. [31] presented an energy and cost trade-off for computational tasks offloading in mobile multi-tenant clouds. Various policies proposed that 5G enabled cloud can employ to solve the general case. Also, the complexity of this proposed heuristic algorithm is elaborated with performance evaluation to attain high performance.

3 Cloud migration

Cloud migration involves shifting applications and data hosted in a local architecture to a scalable environment in cloud. Cloud migration enables access to services over the internet. There are many clouds migration practices for business enterprises, but all of them possess distinct features and migration methods [32]. The most adopted models for cloud migration are the ‘lift and shift’ and the ‘cloud-to-cloud’. In the context of the present work, we will focus on cloud-to-cloud (C2C) migration with the following key benefits:

Scalability as the business demands, they could scale up and down.

Mobility users can request the essential service and launch via any connected devices anywhere.

Affordability cloud-based services are available at a cheap cost with offerings such as pay-as-you-go.

Security transactions across the cloud environment wrapped with strict security measures.

Measurability without any shortage or shed-load, it provides measured services as per the business requirements and requests adequate service on demand.

3.1 Cloud migration threats

Although there are numerous benefits for cloud infrastructure, there are several threats as well associated with cloud-based applications and data. The newer versions of a protocol such as TLS are less vulnerable than SSL, but TLS had security issues. The DROWN (decrypting RSA with obsolete and weakened encryption) attack disrupts the secured communication extended by SSL and TLS. As a result, there is a chance of malicious access to secured data from an unsuspecting server [33]. Figure 1 shows the schematic of DROWN. Although the DROWN infiltration does not provide the hacker with the visibility of the reaction of the malicious incident, nevertheless, it can incur damage.

Since 2011 another form of malicious activity got detected by security experts, which are known as the browser exploit against SSL/TLS, BEAST [34]. BEAST utilizes the cypher block chaining vulnerability in TLS 1.0 to decipher messages. Since TLS 1.0 is now outdated, the chances of BEAST attack is limited to old systems using TLS 1.0. Once in the year 2020 TLS 1.0 is deprecated, the BEAST attack on secured networks will reduce. To avoid such an attack, advice is to use a higher version of TLS. In one of the published articles for 2020 by Acunetix [34], 30.7% of web servers are running with the TLS 1.0 version. This attack will lead to the potential risk of the BEAST attack. There are few more malicious vulnerabilities such

Fig. 1 DROWN (decrypting RSA with obsolete and weakened encryption) attack breaks the communication encryption provided by SSL and TLS

as timing attacks, 2013, crime and breach. browser reconnaissance and exfiltration via adaptive compression of hypertext (BREACH) [35]. Lastly, for completeness, it is worthwhile to mention about Unholy PAC malicious incident that occurred during 2016. PAC takes advantage of the limitation of the web proxy auto-discovery protocol (WPAD). The impact of WPAD is that it makes the URL visible, even though the user might be accessing it via a secured tunnel of TLS [36].

3.2 Cloud to cloud migration

C2C migration involves the transfer of information technology-related environment seamlessly from one cloud (source) to another cloud (destination). C2C migration provides an entity to change cloud service providers without the intermediate step of migrating data to an in-house environment [37]. One of the most critical aspects of the selection of a cloud service provider is its capability to facilitate ease of cloud migration. In a multi-cloud data migration scenario, the complications further increase. Currently, there are well-thought processes, capable tools to facilitate C2C data migration with minimum risk. The objective of C2C migration is to leverage the benefits associated with the host environment's IT infrastructure capability and security. Further, C2C migration aims to achieve benefits such as flexibility, easy service provisioning, and a pay-per-use model [38].

Figure 2 shows a C2C migration. The process of migrating from one cloud infrastructure to another cloud platform involves multiple considerations such as migration of the web layer, application layer, and databases.

While migration, there are three types of communication channels that are used. The purpose of C2C is authenticated access by users and trusted third parties to manage and control the C2C migration process. To ensure that there are no mismatches in source and destination cloud capabilities [39]. This channel is required to rehearse migrations multiple times to make sure that everything is successful before doing a production cutover. A detailed migration document needs to be in place for validation with a master migration checklist. The next channel is a dedicated VPN tunnel established for real-time high demand transfers. The VPN is using state of the art routers and standard protocols such as TLS [40]. VPN can be a node-to-node network such as multiprotocol label switching (MPLS) which, employs a range of access technologies like T1/E1, ATM, frame relay, and DSL. MPLS directs data from one node to the next based on a short path. The third channel is the backend replication channel. VPN implemented using an internet access gateway. Mostly archival data, scheduled back up, DR (disaster recovery) data replicated using this channel [41].

3.3 Digital identity models

There are three digital identity models—Siloed, third part identity provider, and self-sovereign. Figure 3 shows the comparison of three models.

The first model is Siloed—system issued a digital identity credential to use its facilities. Every user needed a new digital identity credential for every new application. Siloed led to a poor user experience. The second model of digital identity is called the Federated one. In this model, a

Fig. 2 Schematic diagram of cloud-to-cloud migration involving a source cloud and a destination cloud environment

Fig. 3 Three digital identity models—Siloed, third part identity provider, and self-sovereign

third-party provider provides user credentials, such as the “Login with LinkedIn” functionality. With this model, LinkedIn became the middleman of trust. The emergence of blockchain technology, decentralized identifiers, and verifiable credentials allowed the creation of a third model of identity: self-sovereign identity.

3.4 Self-sovereign identity model

The data security control is by several applications and services that receive access consent from end-user. This condition is risky because these centralized organizations are increasingly prone to malicious attacks and impersonation [42]. A digital identity consists of information about the online credential of an entity. Self-sovereign identity is an approach to allow online entities to regain control for the authorization of credentials. In essence, this approach to encrypted digital identity data in a cloud hub is to be accessed by an authorized entity. Through this process, an entity can get rid of the need for providing general consent to multiple platforms and applications [43]. One of the benefits is that one can revoke the access credential if there is a trust issue with the application or platform. Following are the prerequisites for the use cases where SSI can be useful:

Cloud infrastructure should have a system with a database.

Multi-user concurrent update to the database.

The users need to trust each other.

There is a problem in using the third party provided services. The data transaction for the deployed cloud applications is dependent on each other.

SSI’s main aim is to build trust by reducing dependency on mutually trustworthy agents between source and destination. By elimination of the third party in between for validation will enable faster transaction and optimization of audit process and steps. As a tangible outcome, this will

lead to cost reduction through the decentralization of the process [44]. Figure 4 shows the updated C2C migration diagram with the replacement of a trusted third party by an encrypted digital hub for SSI implementation. SSI extends traces of malicious activity records for future reference. As can be seen, the digital hub is replicate with each router. SSI streamlines administrative overheads, optimizes the cost of ownership, automated periodical update, and access to any end-user. This approach reduces the risk of man inflicted errors associated with trusted third-party processes [45]. Further, the benefits are bi-directional asynchronous workflow control. An effective wide range of access system key management enables any public keys type and format, highly available, scalable, the reduced cost with automated less complexity backup and recovery process.

3.5 SSI platform security

Present SSI platform security for C2C migration includes TLS during the communication between peer to peer. TLS communication protocol has evolved from erstwhile SSL protocol [46]. Another critical component of the security platform is encrypting/signing the communication packet of the data while transport data from peer to peer. TLS ensures end to end security. TLS is a complex protocol and includes operations such as transport and session layers. TLS involves cryptography and relies on the X.509 certificate. The PKI framework includes partner authentication, legitimation, and revocation [47]. Another aspect of the TLS protocol is its asymmetrical behavior while communicating between two computers. The server-side computer is responsible for authentication, presents its X.509 certificate, and is highly dependent on the PKI framework. The client-side computer acts anonymously [48]. We propose a public key infrastructure scheme for providing bidirectional authenticated and encrypted communication as well as host-level access controls between services achieved using TLS. With the new approach, both the

Fig. 4 C2C migration with encrypted digital hub replacing trusted third party

client and server possess certificates. Mutual TLS extends the server to authorize the credibility of the client before establishing a connection [49]. By including information about a host in its certificate, servers can determine the identity of a requesting server and perform access controls accordingly. For instance, the system can enforce that only servers during C2C migration are allowed to perform the decrypt operations and that these servers may only perform an operation using private keys. Figure 5 shows the proposed SSI based platform security model for C2C migration [50].

Every instance in the proposed platform is with a security certificate. The certificate is either a client or server certificate. The certificates are issued by a certificate authority and have validity as defined by the duration of the C2C migration. Authentication from an encrypted digital hub is using the authentication process [51].

3.6 Rivest Shamir Adleman algorithm (RSA)

Cryptographic algorithms are essential to realizing the data security system. In current work, one of the popular algorithms called Rivest Shamir Adleman (RSA) is using for encryption. RSA uses asymmetric algorithms with the key pair for encryption and decryption. The security key size of the password is critical for the quality of the security of the algorithm. If the security key size is small, there is a higher possibility that the combination of locks can unlock by brute force attack (BFA). BFA uses the steps of assessing the combination of the one-by-one key to decipher the actual key. There are multiple research going on which established that the prime numbers created in the RSA impact the password key size [52–55]. Figure 6 shows the diagram of RSA algorithm-based Encryption and decryption. The unique part of RSA is that the data encryption is by the public key. To decrypt the private key is required.

Fig. 5 Proposed SSI based platform security model for C2C migration

Fig. 6 RSA Algorithm based encryption and decryption

The RSA encrypts data packets using a public key. This process does not require to communicate a separate secret key. Often this process is helpful to sign a message.

3.7 Key generation: algorithm

For an authorized cloud user, it is risky to transmit data without encryption. For secured C2C migration, the use of encryption and decryption is essential. The prime numbers generated by the RSA must be kept confidential. Any breach of trust in sharing the prime number of the data may be prone to malicious attacks such as a chosen-ciphertext attack. While the implementation of RSA, the user creates a public key based on two large prime numbers p and q . Further, an auxiliary value n of the form pq enables enhanced secrecy taking advantage of the modulus switching.

3.8 RSA encryption and decryption scheme

Encryption rule

Ciphertext c can be represented as in Eq. 1.

$$c = \text{RsaPublic}(m) = m^e \bmod n, \quad (1)$$

where $1 < m < n - 1$.

Decryption rule

Plaintext m can be represented as in Eq. 2

$$m = \text{RsaPrivate}(c) = c^d \bmod n. \quad (2)$$

Inverse transformation

$$m = \text{RsaPrivate}(\text{RsaPublic}(m)). \quad (3)$$

Signing

Signature s can be represented as

$$s = \text{RsaPrivate}(m) = m^d \bmod n, \quad (4)$$

where $1 < m < n - 1$.

Verification

$$v = \text{RsaPublic}(s) = s^e \bmod n. \quad (5)$$

Inverse transformation

$$m = \text{RsaPublic}(\text{RsaPrivate}(m)). \quad (6)$$

The inverse transformations for encryption and signing are equivalent, since

$$\begin{aligned} \text{RsaPrivate}(\text{RsaPublic}(m)) &= (m^e \bmod n)^d \bmod n \\ &= m^{ed} \bmod n, \end{aligned} \quad (7)$$

$$\begin{aligned} \text{RsaPublic}(\text{RsaPrivate}(m)) &= (m^d \bmod n)^e \bmod n \\ &= m^{ed} \bmod n. \end{aligned} \quad (8)$$

So, we only need to show that the decryption rule works; that is, for (n, e) as defined above, If $c = m^e \bmod n$ for $0 < m < n$ then $m = c^d \bmod n$, where d is the secret exponent that satisfies the relation $ed \equiv 1 \pmod{\phi(n)}$. In summary, how RSA works funnel down to the fact that for any integer x ,

$$x^{1+k\phi(n)} \equiv x \pmod{n}. \quad (9)$$

4 Simulation

A codebase is developed based on the algorithm mentioned in Sect. H. The simulation process involves running the developed code for the following scenarios:

Key generation,
Encryption,
Decryption.

The key configuration parameters considered for simulation are $\phi(n)$, d , p , q , n , e . Based on Eqs. 1 to 9 the developed code uses the configuration parameters to execute different scenarios.

5 Key implementation

Following Eq. 9 the public and private keys are generated for plain text TIGERQU as shown in Table 1.

Table 1 Generated keys for TIGERQU

Parameter	Values
k	5
e	7
p	51
q	5
n	255
$\phi(n)$	200
d	143
Public key 259, 7	
Private key 259, 143	

6 Results and discussion

Table 2 shows the ASCII values post implementation of RAS algorithm and corresponding ASCII values for characters.

Figure 7 shows the block diagram for cloud apps' public and private key generation, encryption of data, and session for the applications using the public key. Once the data and sessions are encrypted, the migration can take place using background or foreground replication. The online access key generators publish public keys for authenticated users to do encryption.

Figure 8 shows the public key generated for data encryption during C2C migration.

Figure 9 shows the private key generated for data decryption during C2C migration.

Figure 10 shows the context test data for encryption testing during C2C migration.

Figure 11 shows the encrypted context test data after encryption testing during C2C migration.

Figure 12 shows the keys generated using online app.

Figure 13 shows the validation using online app.

Table 3 shows the C2C migration performance using automated SSI authentication and TLS for background replication.

Table 4 shows The C2C migration performance after setting up foreground replication channel using SSI and TLS.

Figure 14 shows the C2C migrated file size using automated SSI authentication and TLS for background replication.

Figure 15 shows the C2C migration time taken using automated SSI authentication and TLS for background replication.

Figure 16 shows the C2C migration time taken using automated SSI authentication and TLS for foreground replication.

Figure 17 shows the C2C migration size of files transferred using automated SSI authentication and TLS for foreground replication.

Table 2 ACSII vs. encryption and decryption for TIGER

Character	ASCII	Encrypted	Decrypted
T	84	84	84
I	73	112	73
G	71	11	71
E	69	69	69
Q	81	21	81
U	85	85	85

7 Comparative analysis

Table 5 shows the comparison of C2C migration performance using RSA and TLS vs published result [56, 57] using MDM and TPA methods. According to published information, TPA module consumes less time to encrypt and decrypt data compared to the MDM module.

From the comparison it is evident that SSI based implementation can provide 13.32 Kbps encryption/decryption rate which is significantly higher than TPA method of 1 Kbps.

8 Strength and weakness of SSI method

Following are the strengths and weaknesses of the proposed SSI.

Strength

- Convenience in use,
- Cost reduction,
- Better service delivery,
- Reduction of transaction time,
- More secured.

Weakness

- Attackers may target the nodes implementing SSI.

9 Conclusion

SSI is a combination of multiple technological breakthroughs that have evolved over the years. Trustworthy secured point-to-point communications across entities and gadgets are on the verge of revolutionizing digital media, daily life, work-life and social life. One of the most pressing problems for digital communication over the internet is authentication problems such as identity theft, phishing, etc. Through mutual cryptographic authentication, achieve the IT audit requirements of the privacy norms. Cloud service providers like Amazon EC2, GoGrid, Nephoscale, Google provides API to access and control C2C migration. This paper is more focused on establishing that SSI is a trustworthy approach. The motivation is from the fact that Siloed and IDP models are now obsolete, and the SSI holds the key to a better user experience. A TPA-based security service over the cloud has its challenges. During the recent COVID-19 pandemic, the same surfaced explicitly as available resources are scarce. With the overwhelming progress for cloud-based services, there is a demand for a semi to fully automated SSI implementation to reduce cost and TPA dependencies. With this background, it's essential to manage cloud data strategically

Fig. 7 C2C migration data and session encryption

```
MIGfMA0GCsGqGSIB3DQEBAQUAA4GNADCBiQKBgQDMNV0Qh2ThIY0lCSMAkBX1NsYdpU+DiAvPMMIN23mpYb221Xs5hNyYznTbKA2uxZAvbcZje4t6vSk+qx1a loczJEVBUBWs4nLvCi49Q3RXL3sFq39P35Ze/9PZADV QG0gsJa9zGKlzSI6zji6xhh0gpRIHr555jWqOhT/MvTrp QIDAQAB
```

Fig. 8 C2C migration public key for data and session encryption

```
yqayhrh7RmpEqAjsQMtk4Gu18EnldSh3WQhLdOW1OdJDXMrTAafIJ7qSC1RMMqUNfEG+eFD+4bkplx2agIMdkCt7o+whyNqHKQPA0KLffJw9i+cy7JlZPXRMIJbyTAdjQc6MIYyJyLcULUArn6fyKnU4xCfY1z4Lt+A AFOWGTI=
```

Fig. 11 C2C migration context data after migration

```
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBAMw1XRCHZOEHjSVxIwCQHUU2xh2IT4OIC88wyU3bealhvvbVezmE3JjOdNsoDa7FkC9txmN7i3qKT6rHVqWhzMkRUFYRgZicu8KLj1DdFcvewWrf0/fll7/09kAO9AbSCwlr3MYqXNljrOOLrGGGHSCIEgevnmmNao6G38y9OulAgMBAAECgYAbMifBqaVe7G60q4mzi3yehrp+PAKISb3sVE8UpqyWNe/vtD3aZ9NoT+h5oVb3eZCymT93fdGUmVpeLMh2qUJhw63Ken39YyDHRh2/6mZc46q6MAQqYCKV1XMrQpO7auqsOj6nU67t5HkhlG89YlnGcm4ZZbNocSJ6GR3aACQJBAPlvxy1dgsTaL7DOG2BplrbYuEekwU8JLsSLjUNOQe18NdEbVCsHEic+t7MOclmNS4EvS0JOYm4BYC+X2OJq0AsCQQRDIOMZT25EMO56EepgWs+T0eYFebOFJhJEjWUUDcuH7CBME7QPPmLTm4hU5C5jCh8neMoEmjFPYUKCXTDn5hEPAkEAlAo1kogdRJf6FgU9WktQl+QWWu79i9r3Vs88V+YnHVXK2wBNQ/w9YwdmH29DjsK9PT7Ee+XppUBLxfNpVXfvYQJAEqdHV07biJQ2VYUMsEDE4tyvXWNkmAA4dgODsJI9wo6qnTrPtt+dmnoq22Xt1bqSPAQUyaYO9OJR44QRuX/wJAN98asar4x+V+W1CE9Ars+J/QE6cLPh8AsDYbTIGseBIAVXCsSylFAMZ6jVBpx/vNziMF5FQtdRveg+OfpW8cjw==
```

Fig. 9 C2C migration private key for data and session decryption **Fig. 12** C2C migration context data using online app

Hello World

Fig. 10 C2C migration context data during migration

RSA Encryption

Enter Plain Text to Encrypt
Hello World

Enter Public/Private key
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC0MNV0Ch2HtY0icSMaKBNiNsYdpU+DIAvP
MkMhZ3mpYs22Xs8HyZnTBKA2usZAvbczje4
t6vSk+qx1alocZJEVBUBW84nLVCi49Q3RXL3sfq3
9P35Ze/9PZADvQGOgsJa9zGkzSi6ji6xhnh0gp
RHR55jWqQht/MvTtpQIDAQAB

RSA Key Type: ☒ Public key ☐ Private Key

Select Cipher Type
RSA/ECB/PKCS1Padding

Encrypt

Encrypted Output (Base64):
naWCmtVr8JW9B418Eqnlp0LSYkpcokY8x60Pj
/hHgmQyJ6vK/Gi+oB4cgOPDLNn4A3JLWV/c
heaafcJBoqfs/rllC8pvrUIZFoJLQFOPTFIM8yh
mBLU7gm8UeyM9TMkMxziHz/yvp2r1BBP/KycJl
rDDEbO7op9ot9i=

RSA Decryption

Enter Encrypted Text to Decrypt (Base64)
naWCmtVr8JW9B418Eqnlp0LSYkpcokY8x60Pj
/hHgmQyJ6vK/Gi+oB4cgOPDLNn4A3JLWV/c
heaafcJBoqfs/rllC8pvrUIZFoJLQFOPTFIM8yh
mBLU7gm8UeyM9TMkMxziHz/yvp2r1BBP/KycJl
rDDEbO7op9ot9i=

Enter Public/Private key
QGHSCEIgevnmmNao6G38y9CulaGmBA
AECgYABMfBQave706G4mzi3yehrp+P
AKistb3vEBUpqyWnc/vtD3aZ9NoT+h5
oVb3eZcymT83iGUmVpeLmH2qUJhw6
3ken38YvYdHR9/6mZc48qBMAQqyCK
VVIXMrQpO7auqsQj6nu67t5HkHqB89Vn
OCm4ZzbNocSJ6GR3aACQJBAFVyxldg
tTol7ODG2BpbyuEekvU8JLSUJN0qE1
8NDEbVCSHic+T7MOclmNS4EvS0J0ym
4BYC+X2OJqGAScQQRiOmZT25EMO56
EppgWw+TcWfFeOFJhJEJWUUDcuH7C8
ME7QPPmLTm4nHUSJC8Nme8mJpV
UKCXTDn5HEPAKEAIAokogdRjF6FgU9Wk
tQI+QWwU79i9r3v88V+YrhVXK2wBNC
/w9YvdmH22QjK9P7Te+XppJULxRpV
XfVYQJAEqGHV07bJQZVVMSEDE4tyvX
WNkmAA4dgODsJf6wo8qntTPT+dmno
q22Xt1bqSPAWQuayYO9QUR44Q8uX/wJ
ANB8scsr4s++WICE8Ate+J/Q8GcP8B
AsDyBTGSeBIAVXcsSYIAMZ6jV8pX/vNzi
MFSqtdRveg+OfpW8cjw==

RSA Key Type: ☐ Public key ☒ Private Key

Select Cipher Type
RSA/ECB/PKCS1Padding

Decrypt

Decrypted Output:
Hello World

Fig. 13 C2C migration online validation

and provide the required protection. Each stage of the C2C migration process demand to be secured. This work is an attempt to replace TPA with SSI. A cryptographic technique for secured C2C migration using SSI was implemented. SSI is used to facilitate peer-to-peer transactions without the need for TPA. Post-implementation, we have analyzed the C2C performance and found in most of the replication scenario (background or foreground) is

achievable. Mathematically computed encrypted and decrypted ASCII values for the word “TIGERU” matched the output by the algorithm. Also, the keys generated using the algorithm are validated with an online validator to ensure the correctness of the access key generation of the algorithm. From the result of the implemented algorithm, it is proved that SSI based implementation can provide a 13.32 Kbps encryption/decryption rate which is significantly higher than the TPA method of 1 Kbps. SSI proposes sovereignty for the individual not in the issuance but the management of their identity and reduced TPA dependencies. We can conclude that RSA based mutual TLS can be a candidate for SSI based C2C migration for reduced cost and a highly safe environment. We recommend optimized RSA based automated certificate services driven by the latest standards. This approach will eliminate the risks associated with proprietary and outdated interfaces in premises or cloud environments and create a cost-effective homogeneous C2C migration environment.

10 Future

The use of SSI based data migration is in the early stage of adoption but has great potential. This is because the approach enables sovereignty for individuals over their digital assets and credentials. The portability of digital documents like certificates, passports, property titles, and

Table 3 C2C migration performance—background replication

File type	Number of files	Average file size (MB)	Total file size (GB)	Compression (%)	Total size uploaded (GB)	Average file/hour	Time (h)
Database	8515	54	460	1	457	203	42
Documents	2549	212	540	1	537	65	39
Applications	51	201	10	0	10	73	1
Image	3000	221	663	0	660	69	44
Audio	1000	191	191	0	190	77	13

Table 4 C2C migration performance—foreground replication

File type	Number of files	Average file size (MB)	Total file size (GB)	Compression (%)	Total size uploaded (GB)	Average file/hour	Time (h)
Session	1500	0.48	0.7	0	0.72	250	6
Codes	1700	1	2	1	2	45	38
Scripts	700	1	1	0	1	45	16
Config files	400	0.5	0.2	0	0.2	42	10

Fig. 14 C2C migration performance for background replication **Fig. 15** C2C migration background replication—time **Fig. 16** C2C migration performance for foreground replication—time taken **Fig. 17** Foreground replication—file size upload

digital wallets using mobile apps will become more trustworthy because of the non-mediation of a TPA. The basic essence is to prove the ownership, the owner does not need to reach out to the issuer to verify them. Another evolving area is the integrated security approach with 24/7 cloud security monitoring. Organizations need today to protect their data and users in real-time. Cloud security providers that can comply with GDPR, the toughest privacy and security law in the world will be in high demand over the coming years.

Table 5 C2C migration performance—comparison

Method	Duration (s)	Size (KB)	Encryption/decryption rate (Kbps)
MDM	350	347	0.99
TPA	250	249	1.00
RSA and TLS	249,285	3,320,000	13.32

Funding This work was supported by the Universiti Kebangsaan Malaysia (UKM) under the Research Grant Ministry of Education Malaysia, FRGS/1/2020/ICT03/UKM/02/6.

Declarations

Conflict of interest The authors declare no conflict of interest.

References

- Housley, R., et al.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL). <https://www.ipa.go.jp/security/rfc/RFC3280-00EN.html>. Accessed 01 Jan 2021
- Perl, H., Fahl, S., Smith, M.: You won't be needing these any more: on removing unused certificates from trust stores. In: International Conference on Financial Cryptography and Data Security. Springer, Berlin (2014)
- DigiNotar removal follow up (2011). <https://blog.mozilla.org/security/2011/09/02/diginotar-removal-follow-up>. Accessed 01 Jan 2021
- Hasan, M.K., Ahmed, M.M., Hashim, A.H., Razzaque, A., Islam, S., Pandey, B.: A novel artificial intelligence based timing synchronization scheme for smart grid applications. *Wirel. Pers. Commun.* **114**(2), 1067–1084 (2020)
- Hasan, M.K., Ismail, A.F., Abdalla, A.H., Abdullah, K., Ramli, H., Islam, S., Saeed, R.A.: Inter-cell interference coordination in LTE-A HetNets: a survey on self organizing approaches. In: 2013 International Conference on Computing, Electrical and Electronic Engineering (ICCEEE), 26 August 2013, pp. 196–201. IEEE (2013)
- Hasan, M.K., Ismail, A.F., Islam, S., Hashim, W., Ahmed, M.M., Memon, I.: A novel HGBBDSA-CTI approach for subcarrier allocation in heterogeneous network. *Telecommun. Syst.* **70**(2), 245–262 (2019)
- Hasan, M.K., Saeed, R.A., Hashim, A.H., Islam, S., Alsaqour, R.A., Alahdal, T.A.: Femtocell network time synchronization protocols and schemes. *Res. J. Appl. Sci. Eng. Technol.* **4**(23), 5136–5143 (2012)
- Amanlou, S., Hasan, M.K., Bakar, K.A.: Lightweight and secure authentication scheme for IoT networks based on publish-subscribe fog computing model. *Comput. Netw.* **199**, 108465 (2021)
- Hasan, M.K., Shafiq, M., Islam, S., Pandey, B., Baker El-Ebiary, Y.A., Nafi, N.S., Ciro Rodriguez, R., Vargas, D.E.: Lightweight cryptographic algorithms for guessing attack protection in complex Internet of Things applications. *Complexity* (2021). <https://doi.org/10.1155/2021/5540296>
- Akhtaruzzaman, M., Hasan, M.K., Kabir, S.R., Abdullah, S.N., Sadeq, M.J., Hossain, E.: HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey. *IEEE Access* (2020). <https://doi.org/10.1109/ACCESS.2020.3040083>
- Hasan, M.K., Islam, S., Sulaiman, R., Khan, S., Hashim, A.H., Habib, S., Islam, M., Alyahya, S., Ahmed, M.M., Kamil, S., Hassan, M.A.: Lightweight encryption technique to enhance medical image security on Internet of medical things applications. *IEEE Access* **9**, 47731–47742 (2021)
- Comodo: Comodo Fraud Incident. Comodo (2011). <https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html>. Accessed 01 Jan 2021
- Wendlandt, D., Andersen David, G., Perrig, A.: Perspectives: improving SSH-style host authentication with multi-path probing. In: USENIX Annual Technical Conference (2008)
- Bates, A., Pletcher, J., Nichols, T., Hollembaek, B., Butler, K.R.B.: Forced perspectives: evaluating an SSL trust enhancement at scale. In: Proceedings of the 2014 Conference on Internet Measurement Conference. ACM (2014)
- Khan, S., Zhu, L., Zhang, Z., Rahim, M.A., Khan, K., Li, M.: Attack-resilient TLS certificate transparency. *IEEE Access* **8**, 98958–98973 (2020). <https://doi.org/10.1109/ACCESS.2020.2996997>
- Thaseeb, K., Din, I.U., Almogren, A., Jan, Z., Abbas, N., Adnan, M.: DDR-ESC: a distributed and data reliability model for mobile edge-based sensor-cloud. *IEEE Access* **8**, 185752–185760 (2020)
- Memon, I., Shaikh, R.A., Hasan, M.K., Hassan, R., Haq, A.U., Zainol, K.A.: Protect mobile travelers information in sensitive region based on fuzzy logic in IoT technology. *Secur. Commun. Netw.* (2020). <https://doi.org/10.1155/2020/8897098>
- Moghaddam, J., Esmailzadeh, M., Ghavipour, A., et al.: Minimizing virtual machine migration probability in cloud computing environments. *Clust. Comput.* **23**, 3029–3038 (2020). <https://doi.org/10.1007/s10586-020-03067-5>
- Aruna, M.G., Mohan, K.G.: Secured cloud data migration technique by competent probabilistic public key encryption. *China Commun.* **17**(5), 168–190 (2020). <https://doi.org/10.23919/JCC.2020.05.014>
- Masdari, M., Khezri, H.: Efficient VM migrations using forecasting techniques in cloud computing: a comprehensive review. *Clust. Comput.* **23**, 2629–2658 (2020). <https://doi.org/10.1007/s10586-019-03032-x>
- Ahmad, N., Naveed, Q.N., Hoda, N.: Strategy and procedures for migration to the cloud computing. In: IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), Bangkok, Thailand, pp. 1–5 (2018). <https://doi.org/10.1109/ICETAS.2018.8629101>
- Zhao, D., Luo, L., Yu, H., et al.: Security-SLA-guaranteed service function chain deployment in cloud-fog computing networks. *Clust. Comput.* **24**, 2479–2494 (2021). <https://doi.org/10.1007/s10586-021-03278-4>
- Kumar, D., Singh, R.K., Layek, A.: Block chain and its application. In: Kumar, K., Davim, J. (eds.) *Supply Chain Intelligence. Management and Industrial Engineering*. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-46425-7_6
- Casino, F., Thomas, K., Patsakis, D.C.: A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telemat. Inform.* **36**, 55–81 (2019). <https://doi.org/10.1016/j.tele.2018.11.006>
- Chaudhry, S.A., Yahya, K., Al-Turjman, F., Yang, M.-H.: A secure and reliable device access control scheme for IoT based sensor cloud systems. *IEEE Access* **8**, 139244–139254 (2020). <https://doi.org/10.1109/ACCESS.2020.3012121>

26. Mo, Y., Liang, M., Xing, L., Liao, J., Liu, X.: Network simplification and K terminal reliability evaluation of sensor-cloud systems. *IEEE Access* **8**, 177206–177218 (2018)
27. Ahmed, Z.E., Hasan, M.K., Saeed, R.A., Hassan, R., Islam, S., Mokhtar, R.A., Khan, S., Akhtaruzzaman, M.: Optimizing energy consumption for cloud Internet of Things. *Front. Phys.* **8**, 358 (2020). <https://doi.org/10.3389/fphy>
28. Ghazal, T.M., Hasan, M.K., Hassan, R., Islam, S., Abdullah, S.N., Afifi, M.A., Kalra, D.: Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. *Solid State Technol.* **63**(1s), 2513–2521 (2020)
29. Liang, J., Zhang, M., Leung, V.C.: A reliable trust computing mechanism based on multi-source feedback and fog computing in social sensor cloud. *IEEE Internet Things J.* (2020). <https://doi.org/10.1109/JIOT.2020.2981005>
30. Wang, T., Mei, Y., Jia, W., Zheng, X., Wang, G., Xie, M.: Edge-based differential privacy computing for sensor–cloud systems. *J. Parallel Distrib. Comput.* **136**, 75–85 (2020)
31. Patel, Y.S., Reddy, M., Misra, R.: Energy and cost trade-off for computational tasks offloading in mobile multi-tenant clouds. *Clust. Comput.* **24**, 1793–1824 (2021). <https://doi.org/10.1007/s10586-020-03226-8>
32. Kim, H., Chun, K., Kim, H., Chung, Y.: Utilization of workflow management system for virtual machine instance management on cloud. *Concurr. Comput. Pract. Exp.* **27**(17), 5350–5373 (2015)
33. Zorz, Z.: DROWN attack breaks TLS encryption, one-third of all HTTPS servers vulnerable. *Help Net Security*, 1 March (2016). <https://www.helpnetsecurity.com/2016/03/01/drownattack-breaks-tls-encryption-one-third-of-all-https-servers-vulnerable/>. Accessed 01 Jan 2021
34. Duong, T., Rizzo, J.: Attack against TLS 1.0's use of cipher block chaining (CBC) in a browser environment. *Imperial Violet*. <https://www.imperialviolet.org/2011/09/23/chromeandbeast.html>. Accessed 01 Jan 2021
35. Hijmans, R.J., van Etten, J.: Raster: geographic analysis and modeling with raster data. R Package Version 2.0-12, January 12 (2012). <http://CRAN.R-project.org/package=raster>. Accessed 01 Jan 2021
36. Sankalpa, I., Dhanushka, T., Amarasinghe, N., Alawathugoda, J., Ragel, R.: On implementing a client–server setting to prevent the Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext (BREACH) attacks. In: 2016 Manufacturing and Industrial Engineering Symposium (MIES), Colombo, pp. 1–5 (2016). <https://doi.org/10.1109/MIES.2016.7780263>
37. Dan, G.: New attack bypasses HTTPS protection on Macs, Windows, and Linux. *Ars Technica*, July (2016). <https://arstechnica.com/information-technology/2016/07/new-attack-thatcripples-https-crypto-works-on-macs-windows-and-linux/>. Accessed 01 Jan 2021
38. Zhu, Y., Huang, D., Hu, C.J., Wang, X.: From RBAC to ABAC: constructing flexible data access. *IEEE Trans. Serv. Comput.* **8**(4), 601–616 (2015)
39. Malik, A.M., Khan, S.: DaSCE: data security for cloud environment with semi-trusted third party. *IEEE Trans. Cloud Comput.* (2016). <https://doi.org/10.1109/TCC.2015.2446458>
40. Alsalihi, Y.: An accurate and high-efficient QuBits steganography scheme based on hybrid neural networks. *Multimed. Tools Appl.* **78**, 1–17 (2019)
41. Shs, H., Ding, W.: Cryptanalysis of three dynamic ID-based remote user authentication schemes using smart cards. In: *IEEE International Conference of Online Analysis and Computing Science (ICOACS)*, pp. 44–52 (2016)
42. Szalachowski, P., Perrig, A.: Short paper: on deployment of DNS-based security enhancements. *Financial Crypto* (2017)
43. VanderSloot, B., Amann, J., Bernhard, M., Durumeric, Z., Bailey, M., Halderman, J.A.: Towards a complete view of the certificate ecosystem. In: *ACM ICM* (2016)
44. Varshney, G., Szalachowski, P.: A metapolicy framework for enhancing domain expressiveness on the Internet. In: *Secure Comm* (2018)
45. W3Techs: Usage of SSL certificate authorities for websites (2018). bit.ly/2IoWN8u
46. Wang, Z., Lin, J., Cai, Q., Wang, Q., Jing, J., Zha, D.: Blockchain based certificate transparency and revocation transparency. *IEEE Trans. Depend. Secure Comput.* (2018). <https://doi.org/10.1109/TDSC.2020.2983022>
47. Ouvrier, G., Laterman, M., Arlitt, M., Carlsson, N.: Characterizing the https trust landscape: a passive view from the edge. *IEEE Commun. Mag.* (2017). <https://doi.org/10.1109/MCOM.2017.1600981>
48. Newton, A.: Cross Registry Internet Service Protocol (CRISP) Requirements. Technical Report, RFC Editor. <https://www.rfc-editor.org/info/rfc3707>. (Status: Informational) (Stream: IETF, Area: app, WG: crisp). <https://doi.org/10.17487/RFC3707>
49. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A.B., Chen, S.: The blockchain as a software connector. In: *Proceedings* (2016)
50. Braga, J., de Amorim Silva, R., Endo, P.T., Omar, N.: Dark think security: enhancing the security for the autonomous architecture over a restricted domain. In: *Proceeding of CSBC 2017*, p. 8. Mackenzie Presbyterian University (2017)
51. Knauth, T., Steiner, M., Chakrabarti, S., Lei, L., Xing, C., Vij, M.: Integrating remote attestation with transport layer security. *CoRR* (2018). <http://arxiv.org/abs/1801.05863>
52. Elkhail, A., Zhang, J., Elhabob, R.: An efficient heterogeneous blockchain-based online/offline signcryption systems for Internet of vehicles. *Clust. Comput.* **24**, 2051–2068 (2021). <https://doi.org/10.1007/s10586-021-03246-y>
53. Ji, Y., Shao, B., Chang, J., et al.: Flexible identity-based remote data integrity checking for cloud storage with privacy preserving property. *Clust. Comput.* (2021). <https://doi.org/10.1007/s10586-021-03408-y>
54. Rashid, A., Masood, A., Khan, A.U.R.: RC-AAM: blockchain-enabled decentralized role-centric authentication and access management for distributed organizations. *Clust. Comput.* (2021). <https://doi.org/10.1007/s10586-021-03352-x>
55. Rabaninejad, R., Rajabzadeh Asaar, M., Ahmadian Attari, M., et al.: An identity-based online/offline secure cloud storage auditing scheme. *Clust. Comput.* **23**, 1455–1468 (2020). <https://doi.org/10.1007/s10586-019-03000-5>
56. Elhabob, R., Zhao, Y., Eltayieb, N., et al.: Identity-based encryption with authorized equivalence test for cloud-assisted IoT. *Clust. Comput.* **23**, 1085–1101 (2020). <https://doi.org/10.1007/s10586-019-02979-1>
57. Dewan, S., Kumar, D., Gonnade, S.: Secure data migration across cloud system using third party auditor (TPA). *Int. J. Innov. Res. Sci. Eng. Technol.* (2015). <https://doi.org/10.15680/ijirset.2015.0406031>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

experience.

M. G. Aruna is a Faculty of MSEC and Research Scholar of SVIT, affiliated to Visvesvaraya Technological University, Belagavi, India. She has completed her B.E. and M.Tech. from Bangalore University and Dr. from MGR University. Her research interest is databases, networks and data security, Internet of Things, machine learning, and cloud computing. She has overall 17 years of experience as an academican and 7 years of research

Mohammad Kamrul Hasan, SM'17 is currently working as a Senior Lecturer in the Network and Communication Technology Research Cluster, Center for Cyber Security, Universiti Kebangsaan Malaysia (UKM). He completed a Doctor of Philosophy (Ph.D.) Degree in Electrical and Communication Engineering from the Faculty of Engineering, International Islamic University, Malaysia, in 2016. Dr. Hasan completed his M.Sc. Degree in Communica-

tion Engineering from the Department of Electrical and Computer Engineering, International Islamic University, Malaysia, in 2012. Dr. Kamrul is a Senior Member of the Institute of Electrical and Electronics Engineers since 2013, a Member of the Institution of Engineering and Technology, and a Member of the Internet Society. He has served the IEEE IIUM Student Branch as Chair from 2014 to 2016. He is a Certified Professional Technologist and consulting the related industries. His research interest includes telecommunications, Internet of Things, vehicular networks, smart grid technologies, microprocessor and interfacing, and cyber-physical security.

Shayla Islam (M'16) is currently working as an Assistant Professor in UCSI University, Malaysia. She has completed Ph.D. Degree in Engineering from Electrical and Computer Engineering Department, International Islamic University Malaysia (IIUM) in 2016 under Malaysian International Scholarship (MIS). She completed her M.Sc. at the Department of Electrical and Computer Engineering in International Islamic University Malaysia in 2012.

Dr. Shayla is a Member of the Institution of Engineers Bangladesh (MIEB-M/40624) and Graduate Technologist of the Malaysia of the Board of Technologists (GT19120190). Her current research interests include data communications and networking, computer networks and wireless communication, network mobility in heterogeneous network, computer architecture and cloud computing. She published more than 70 papers in international journals and conferences (WoS/ISI/ESCI

and Scopus indexed). She works as a reviewer for many international conferences as well as journals. Her research interest includes network mobility, vehicular communication systems, cyber security, artificial intelligence and information centric networks.

K. G. Mohan is working as Professor of CSE at GITAM University. He received a Ph.D. from Anna University in 2007 in the Domain of Computer Architecture. His working area of research interest includes low power architecture design, cloud computing, WSN, Internet of Things, data and network security, etc. He has overall 34 years of experience as an academican and 16 years of experience in research. He has published a paper in many international

journal and conferences.

Preeta Sharan obtained her Master Degree from Banaras Hindu University and Ph.D. from IIT Bhu, Varanasi. Additionally she did her Post Doctorate from IIT Kharagpur in the Domain of Optical Sensor. She has published many papers in reputed journals and conferences. She has visited many countries for the research papers presentation in the domain of nano-photonics, optical sensors and quantum dots. She is currently working as Professor and

Research Head in Department of ECE, Oxford College of Engineering Bangalore. She has taken various funded projects from government of India. Her area of research includes integrated optics, surface plasmonic resonance, fiber Bragg grating, quantum dots etc. She has taken Membership of technical body like IEEE, ISTE, IETE and IMAPS. She is also the SIGHT Coordinator of IEEE Bangalore Section, India.

Rosilah Hassan (SMIEE-92468479, Ts, Dr.) is an Associate Professor at Universiti Kebangsaan Malaysia (UKM) in the Faculty of Information Science and Technology. She received her Ph.D. in Mobile Communication from the University of Strathclyde, United Kingdom, in May 2008. She obtained her Master of Electrical (M.E.E.) Engineering in Computer and Communication from the UKM, Malaysia, in 1999. Her first Degree was

B.Sc.. in Electronic Engineering from Hanyang University, Seoul, South Korea. Rosilah Hassan worked as an Engineer with Samsung Electronic Malaysia in Seremban, Malaysia before joining UKM in 1997. Besides being a Senior Lecturer, she got experience in management post for the university as the Deputy Director of Academic Entrepreneurship for over seven years. She also is the Head of the

Network and Communication Technology (NCT) Lab in her Faculty. Her research interests are in wireless communications, networking, IoT, and Big Data. She has had experience as an External Examiner

for Master and PhD for both national and international level. She is also an active Member of IEEE, Malaysia Society for Engineering (MySET), Malaysian Board of Technologists (MBoT), and IET.

Authors and Affiliations

M. G. Aruna¹ · Mohammad Kamrul Hasan² · Shayla Islam³ · K. G. Mohan⁴ · Preeta Sharan⁵ · Rosilah Hassan²

✉ Mohammad Kamrul Hasan
mkhasan@ukm.edu.my; hasankamrul@ieee.org

✉ Shayla Islam
shayla@ucsiuniversity.edu.my

¹ Department of Computer Science and Engineering, M S Engineering College, Bengaluru, Karnataka 562110, India

² Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, UKM, 43600 Bangi, Selangor, Malaysia

³ Department of Computer Science, Institute of Computer Science and Digital Innovation, UCSI University, 56000 Kuala Lumpur, Malaysia

⁴ Department of Computer Science and Engineering, GITAM University, Bengaluru, Karnataka 560064, India

⁵ Department of Electrical and Communication Engineering, The Oxford Engineering College, Bengaluru, Karnataka 560064, India